bitsquare

The decentralized bitcoin exchange

Version 1.0

Motivation

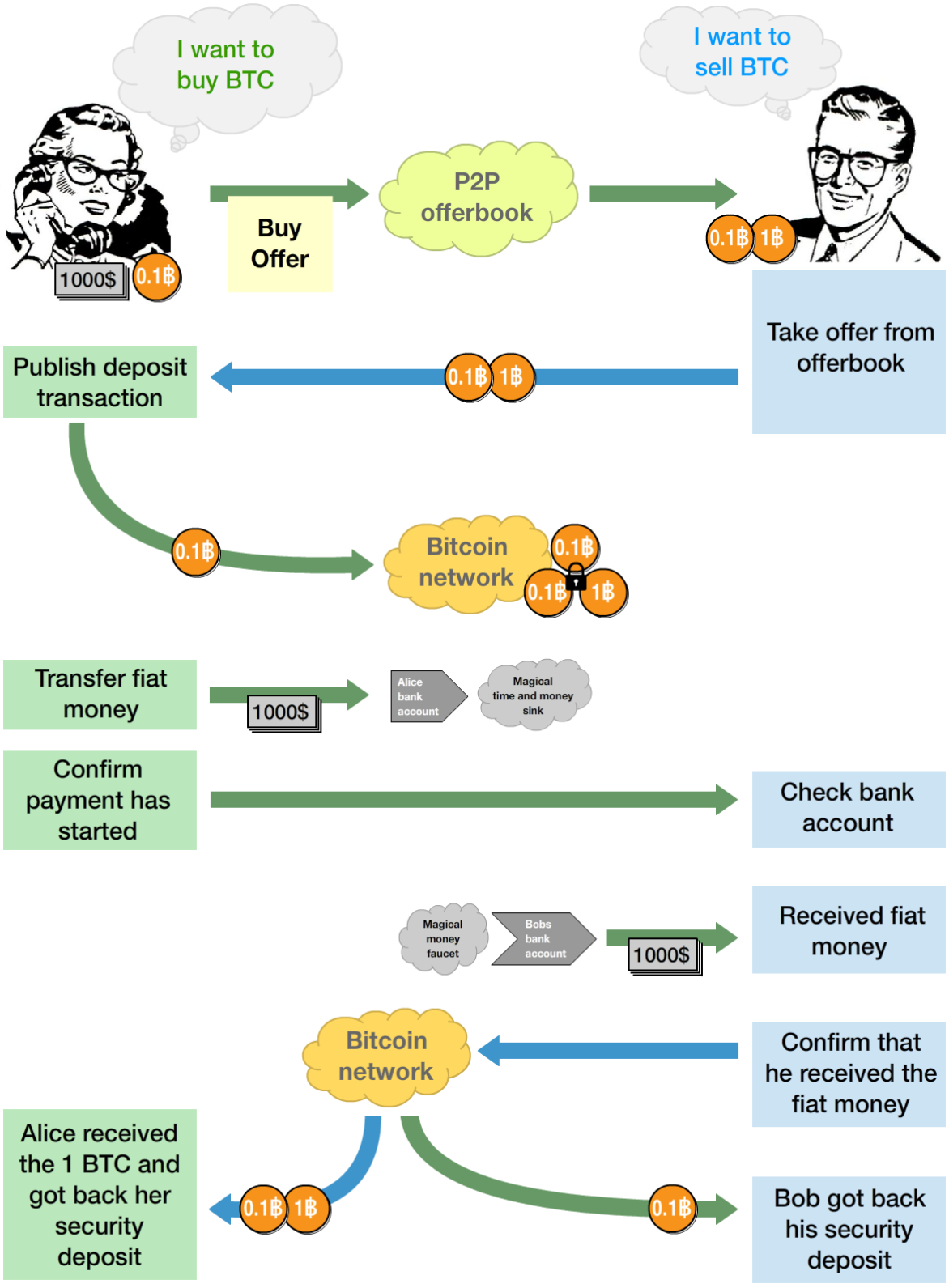
Satoshi Nakamoto created Bitcoin with the motivation to solve the problems of centralized payment systems so it seems inconsistent that centralized Bitcoin exchanges are still the primary way to acquire bitcoin. In our opinion the dominance and vulnerability of centralized exchanges is the Achilles heel in the current Bitcoin ecosystem. There have been many discussions about how to build a pure person-to-person solutions but there is currently no satisfactory solution available.

We aim to develop such a solution based on pure peer-to-peer (P2P) infrastructure.
We cannot prevent the involvement of banks but we can use them in such a way that they are not a conscious and controlling part of the financial transaction. A government can forbid banks to operate with Bitcoin exchanges, but they cannot selectively censor bitcoin related payments between individuals.

Overview

Think of Bitsquare as LocalBitcoins but without a central controlling company, so there is no single point of failure. As mutual trust it not guaranteed between traders we provide several trust mechanisms to make sure both parties fulfill their obligations for each trade. The P2P client software is currently a desktop application (Linux, OS X, Windows) and includes a Bitcoin wallet and uses a secure messaging system with a distributed hash table (DHT) storage protocol. This network infrastructure enables a distributed offer book and the execution of the trade protocol.

This **graphical overview** shows the basic high-level flow of the trade process.



These **videos** demonstrate the current software and give a more detailed explanation of the trade process. A detailed graphical representation of the **trade protocol** should help to explain the way the payment process is executed. A document also discusses the possible **risks, attacks and protection mechanisms**. An **arbitration system** will serve as primary protection mechanism and is also described in a separate document.

Basics

- Pure P2P, no central server, cannot get shut down by a central authority
- National currency will be transferred from one users payment account to the others payment account without any intermediate party.
- Open source, open communication, open development (AGPL)
- Arbitrator system as primary protection mechanism
- Security deposit as additional incentive for honest behavior
- Contract holds all trade details and is signed by both traders, it will be used as evidence in case of a dispute
- Usage of the payment account details in the account registration as scarce resource to prevent sock puppet accounts
- Fraud reports as protection against bank charge backs and crime (stolen payment account)
- Trading fees as protection against spam and market manipulation
- A limit on the trade volume to reduce the overall risk exposure

Limitations

- The duration of the payment transfer limits the speed of the trade process
- Only non-reversible payment transfer methods will be supported (risk of chargebacks)
- Personally identifying information will be leaked between trading partners as part of the payment transfer
- Should not be used in jurisdictions where Bitcoin is illegal (risk from trading with undercover agents)
- You must already have bitcoin to pay small registration and trade fees and for security deposits

Protection

For protecting against several fraud and attack scenarios we use different solutions:

- Security deposit - refundable at settlement
- Arbitrator - a 3rd party that will be used to settle transaction disputes
- Contract - blinded non-refutable proof of trade details used in case of disputes
- Account registration - blinded non-refutable payment account details for mutual verification
- Fraud report - reports by arbitrators with proof of clear cases of fraud
- Trade volume limitation - limits to reduce potential gain from fraud
- Identity verification (optional) - proof of identity confirmed by a trusted arbitrator

Basic use cases

- Register the trading account (include deposit from external wallet)
- Publish an offer (include deposit from external wallet and create offer fee payment)
- Take an offer (includes deposit from external wallet, take offer fee payment and transfer the bitcoin deposit to the escrow account which is a 2 of 3 multi-sig address)
- Make the payment account transfer (out of system; e.g. transfer via online banking webpage)
- Check if payment has arrived on payment account (out of system; e.g. check at online banking webpage)
- Confirm payment receipt and release bitcoin from the escrow account
- Withdraw bitcoin to an external wallet

Extended use cases

- Arbitrator registers and makes security deposit to a 4 of 6 multi-signature (multi-sig) address controlled by top rated arbitrators.
- Arbitrator creates his profile
- Arbitrator leaves and gets back his security deposit
- In a dispute case: Buyer or seller can request arbitration
- In a dispute case: Arbitrator investigates the case out of the Bitsquare system, using methods defined in their profile
- In a dispute case where the buyer is at fault: Arbitrator creates a transaction to refund the seller their bitcoin and security deposit; the buyers security deposit is used to pay the arbitration fee.
- In a dispute case where the seller is at fault: Arbitrator creates a transaction to payout the buyer their bitcoin and security deposit; the sellers security deposit is used to pay the arbitration fee.
- When a dispute is settled by arbitration: signature on refund or payout transaction must be signed by the seller or buyer respectively with the arbitrator also signing.
- When criminal fraud is detected: Arbitrator publishes and signs a report containing all data about the criminal trader to the public fraud list. These reports will only be created in clear cases of fraud like bank chargeback or use of a stolen bank account.

Technology

The Bitsquare application is build in Java 8 with JavaFX for the GUI. For interaction with the Bitcoin block chain the library bitcoinJ is used. For decentralized messaging and storage the DHT library TomP2P is used.

Messaging system

There are two main use cases for the P2P network technology:

- Broadcast offer (public data)
- Messaging between trading peers (private and encrypted)

Additionally the DHT messaging system can be used for network-wide broadcasts like:

- Fraud report update
- Alerts (updates, warnings,...)

Key features of the P2P network technology:

- Highly accessible (NAT traversal, firewalls,...)
- Reliable data storage
- Protect privacy
- Data access protection
- Resistant against spam/flooding
- Fast
- Scalable

Wallet

Bitsquare protects the privacy between trades by separating each trade with a different set of addresses. No address will be used for 2 trades.
To avoid loss of privacy due coin merge when doing the deposit and withdraw from the external wallet, the user has to take care in the scope of the external wallet (e.g. usage of Coin Join solutions).

Wallet key features:

- Manage the key pairs (HD wallet)
- Create regular and pay-to-script-hash (P2SH) transactions
- Sign transactions
- Broadcast transactions
- Add data to a transaction (eg. OP_RETURN)

Registration

Registration stores the blinded payments account data in the block chain. The owner can prove ownership but cannot change or remove the associated data once stored in the block chain. For every additional bank account the user has to make a new registration.

As proof of ownership and identity root we use the wallet key pair used to pay the registration fee. The fee will be the sum of the mining fee and the minimum value (we use 0.0001 BTC instead for the minimum value of 0.0000543 BTC to avoid too fractional values) for the OP_RETURN output which is used for storing the hash of the blinded payment account details data to the block chain. It will be 0.0002 BTC .

We make a transaction from the registration address with a OP_RETURN output script and a 20 byte hash attached.

Embedded data = hash(paymentAccountDetails + secret)

PaymentAccountDetails is the serialized data of the payment account details (e.g. IBAN + BIC + holder name + payment account type).

The secret is used as privacy protection to prevent anyone who knows the payment account data details from looking in the block chain for a matching hash and so find out that this person has registered. The secret will only be revealed to the trading partner during the verification process at the beginning of a trade.

In the verification process the other peer generates a hash from the passed secret and payments details. Peers exchange also their registration transaction ID that they can use to look up and verify that the hash created matches the attached registration data.

If the user is listed in the fraud report then all of their private data will be revealed (payment account details, registration ID). Fraud report listing can only be done by the highest rated arbitrators. The report must document the evidence of fraud and will only be applied in clear cases of an unquestionable scam (bank charge back, stolen payment account, arbitrator fee fraud).

See the "Risk Analysis" document for more details.

Costs of Registration

A **registration fee** will be as low as possible. A higher fee does not give more effective protection against sock puppets and would be a barrier for new users.

A **payment account** can be considered as a scarce resource. Creating a new payment account likely has costs and takes effort and time. There are also not an unlimited number of banks in a country and because banks exchange information between themselves one can not frequently open up new payment accounts without creating suspicion of financial crime (eg. money laundering).

Offer

When Alice creates a new offer she needs to define the amount of bitcoin to buy or sell, the price and a minimum amount she is willing to trade. The other data included in an offer, like the acceptable arbitrators or the acceptable payment account countries, will be derived from the account settings.

To avoid potential collusion between the arbitrator and one of the trading parties the arbitrator will be selected in a verifiable but unbiased way. This will ensure no trader can easily force the selection to one preferred arbitrator.

The selection mechanism is described in the "Arbitration System" document.

Security Deposit

The security deposit will be derived from the arbitration fee which will be used as payment to the arbitrator only in case of a dispute resolution.

The security deposit serves also as an incentive to follow the protocol (e.g. to ensure Bob is not lazy or careless and forgets to release the payout transaction) as well as a mechanism to ensure a dishonest trader is forced to pay the costs for arbitration.

Fees

The fees are necessary for protection against offer book spam, market manipulation and identity harvesting. They are also needed as payment to the arbitrators for their service availability. Arbitrators need to get some compensation for agreeing in advance to arbitrate a trade even in the case the trade is not disputed.

Initially the fees will be kept to a minimum. Later as the trading community grows the fees will be adjusted as needed to make the arbitration system sustainable and to adjust to the level of observed fraud activity.

To make the payment process fast we do not wait for one confirmation for fees. A double spend would be possible but will be difficult and the low fee will be not much incentive to do that.

Here is the overview of the expected fees.

- Account registration fee: 0.0002 BTC (mining fee + minimal value for the OP_RETURN output used for the storage of the blinded payments accounts data in the block chain)
- Create offer fee: 0.001 BTC (paid to the arbitrators, mining fee is included)
- Take offer fee: same as create offer fee (and also paid to the arbitrators)
- Bitcoin mining fee: 0.0001 BTC (An explicit mining fee is included in a transaction three times: Deposit from external wallet, trade, withdrawal to external wallet. So the sum is 0.0003 BTC)

In case of a dispute:

- Active arbitration fee: The security deposit from the dishonest trader will be used for the payment of the arbitrators dispute effort. The arbitrators will be able to define their fees in a given range. The fee will be a flat rate per active arbitration. The size of the trade does not affect the time required to mediate a dispute as the amount of work an arbitrator must perform will be roughly constant even when small amounts of value are exchanged. We expect the arbitration fees will be between 0.1 BTC and 0.5 BTC but ultimately will be set by market competition between arbitrators.

Contract

After offer acceptance and take offer fee payment the offer taker creates and signs the contract. The contract contains all relevant data about the trade, including the payment details, the trading

account ID and message ID of both traders. The contract will be verified and locally stored by both peers and will only be used and needed in case of a dispute. The hash of the contract will be included in the deposit transaction as proof that both parties have accepted the trade details. This process will be automated and does not slow down the trade.

Exchange

The exchange implements the protocol for the trading process.

Protocol

When broadcasting an offer, the offering peer agrees to accept any take-offer request which fulfills the constraints defined in the offer.
The take offer process requires that the Bitsquare application of both traders are running (it can run as a background process). They do not need to be physically present at their computer, but the software needs to be online to react to the take offer request.

The bitcoin buyer needs to wait for at least 1 block chain confirmation (as protection against double spend) before starting the transfer of the national currency.
The bitcoin seller will release the deposit after he has confirmed the receipt of the national currency.

Use case 1: Alice want to buy bitcoin for national currency

Here is a detailed graphical overview of the trade protocol.

Create offer

Alice broadcasts a cryptographically signed offer to buy a set amount of BTC with a specific currency at a set rate. She also has to specify which national currency transfer methods and which registered arbitrators she agrees to use. The offer only reveals a message ID, not any personal information. The offer will be stored publicly in the DHT. The offer storage is access protected so that she is the only one who can remove her offer. There will be a maximum time to live (30 days) for the offer storage in the DHT.

Offer book

At startup every trader loads all offers for his selected national currency from the DHT.
He sees displayed all offers he can take (depending on the preferences and offer restrictions like accepted arbitrators and accepted payment account countries). The not accessible offers will be displayed but shown inactive and informative feedback provided on user interaction why that offer is inaccessible.

The trader can filter offers by various parameters to customize his offer book as well as sorting all relevant table columns.

Take offer

After verification that the offer fee was paid by the offerer, Bob looks up Alice's address in the DHT (currently we use the IP address; we are investigating solutions which protect better the offerers privacy) to establish an encrypted direct communication channel. Bob needs to verify that Alice is the one who signed the offer and Alice confirms that the offer is still available (no other trader has taken the offer in the meantime). The offer will remain in the distributed offer book until an escrow deposit is created and funded by both peers. Bob then needs to pay the take offer fee. Until this point neither peer has revealed any private information to the other peer.

Deposit transaction

The deposit transaction is created using a 2 of 3 multi-signature (multisig) pay-to-script-hash (P2SH) output script to fund the escrow address.
The deposit transaction will be passed for completion and signing via a direct communication channel. Finally it will be published to the Bitcoin block chain by Alice.

The deposit transaction to the escrow address contains:

- Input from Alice: Security deposit + mining fee
- Input from Bob: Security deposit + mining fee + payment
- Output to escrow address: 2*Security deposit + mining fee + payment
- Output to record contract hash: OP_RETURN + hash of contract (20 bytes).

Contract

During the trade protocol a contract will be created, signed by both parties and its hash will be attached to the deposit transaction. It will serve as evidence in case of a dispute. The full contract is stored locally by both traders and only the hash of the contract is stored in the Bitcoin block chain.

Account and fee verification

During the trade protocol both traders verify the others trading account registration, the fee payments and that the other peer is not listed in the fraud report. Fee payments do not require block chain confirmation. We accept the very low risk of double spends to avoid usability problems caused by slowing down the process. There will be a second verification at the end of the trade process where a double spend would be detected and that could be used for local blacklisting.

National currency transaction

After the escrow deposit transaction is published Alice waits for at least 1 confirmation, then she starts the transfer of national currency to the bitcoin sellers payment account (eg. by bank transfer).

Create the payout transaction

Alice creates the payout transaction.

The payout transaction contains:

- Input: Funds from multi-sig escrow address, signed by Alice with her private key (1 of 2 necessary signatures)
- Output to Alice: Security deposit refund + release of payment to Alice
- Output to Bob: Security deposit refund

Alice signs her part and sends the partially signed payout transaction to Bob and tells him that she has started the national currency transfer.

Bob waits until he receives the national currency payment

Bob receives the payout transaction and the message from Alice that she has started the national currency transfer. He will periodically check his payment account until the transaction is complete or a predetermined amount of time has elapsed.

Bob signs and publishes the payment/refund transaction

After receiving the money into his payment account, he signs the payout transaction and publishes it to the bitcoin network.
He gets back his security deposit and can withdraw it to his external wallet.
For Bob all has been successfully completed.

As soon as Bob has published the payout transaction Alice gets a message and as soon the transaction is visible on the block chain she can withdraw the bitcoin payment and the refunded security deposit to her external wallet. For Alice all has now been successfully completed.

Use case 2: Alice want to sell bitcoin for national currency

The opposite situation with Alice as the bitcoin seller works similarly to use case 1. The protocol is slightly different but there are no fundamental changes.

Cancel offer

As long an offer is not taken by another trader the creator of an offer can at any time remove the offer. The offer book will be in sync with the DHT so other traders will not see that offer anymore. The reserved security deposit in the trade wallet will be available for withdrawal to an external wallet. The already paid offer fee is lost.

Dispute

There will be a warning notifications to both traders at the middle of the timeout period if the trade has not completed. As soon the timeout is reached the waiting trader who has not received their payment can contact the arbitrator.
The waiting trader sends a request to the arbitrator with the contract attached and a description of the problem.
The arbitrator has to find a fair solution and per contract terms will contact both traders and perform any other contractually pre-determined due diligence.
After the arbitrator has decided in favor of one trader he will contact the winning party to sign a new payout transaction where he takes the security deposit from the losing party as his dispute payment and the bitcoin payment and security deposit will go to the winning party.

The winning party will have no costs. The losing party will lose his security deposit.
In cases where the problem was caused by external circumstances (e.g. bank has blocked the transfer, etc.), the arbitrator will take half of each security deposits as his payment and refund the rest back to the traders.

More details about the arbitration system can be found in the "Arbitration System" document.

The timeouts for the trade process will be determined by the payment transfer method. For example, up to one week for some national bank transfers may be required or as little as an hour for some electronic payment systems.

Optional identity verification

An **optional** identity verification made by one of the highest rated arbitrators will be provided as an additional security mechanism.

See the "Risk Analysis" document for more information.

Arbitrator

See the "Arbitration System" document for more details.

Reputation system

We don't use a reputation system as it is not needed. We consider reputation systems as not a strong protection mechanism due to self-match trades and a decentralized implementation is problematic.

Fraud reports

A fraud report is used to warn about fraud from bank chargebacks, stolen payment accounts or arbitration fee fraud. The arbitration system can not help in these cases because the bitcoin payment has already been released by the time the fraud is discovered. The fraud report only serves to prevent repeated scam with the same account (account ID, message ID, payment account and holder name).

More details are in the "Risk Analysis" document.

Limitations

In countries where Bitcoin use is illegal it is not recommended to use this platform as it comes with severe risks. Undercover agents could easily find traders by acting as a peer trader.

Banks might also block a payment account if they discover involvement in bitcoin trades. If that risk exists in your national banking environment it is recommended that you open a payment account dedicated to bitcoin trading to prevent the hassles of a primary payment account being blocked.

There will never be 100% safety when using any exchange; the same is true for centralized exchanges or any kind of money transfer for that matter.

To limit potential losses the maximum trading volume will be restricted. For example, a limit of five to ten bitcoin might be considered reasonable. This will help reduce the risk of a stolen bank account being used because only a small amount of the money could be exchanged for bitcoin before the theft is discovered, so the platform is less attractive for criminals.